KaneX

博士研究生

研究方向

- 针对低端硬件设备（如单片机、智能卡）上的轻量级加密的侧信道攻击应用方法。
- 新的统计方法在侧信道攻击上的应用。

教育经历

- **纽芬兰纪念大学** 圣约翰斯，加拿大
  学位：博士，专业：计算机工程 *2014 年 5 月 - 2018 年 12 月*
  - 研究方向：针对加密硬件静态功耗的的侧信道攻击
  - 导师：Howard M. Heys
  - GPA：4.00/4.00
  - 课程：ASIC Design, Industrial Machine Vision
  - 由研究生院与导师共同提供全额奖学金。
- **纽芬兰纪念大学** 圣约翰斯，加拿大
  学位：应用科学硕士，专业：计算机工程 *2012 年 7 月 - 2014 年 4 月*
  - 毕业设计：半同态加密算法的实现
  - 导师：Howard M. Heys 和 Saeed Samet
  - GPA：3.71/4.00，必修课排名年级第三
  - 课程：Computer Architecture, High-Performance Computer Architecture, Advanced Concurrent Programming, Embedded/Real-Time System Design, Advanced Digital Systems 等
- **东南大学** 南京，中国
  学位：工学学士，专业：计算机科学与技术 *2008 年 8 月 - 2012 年 6 月*
  - 活动经验：校艺术团合唱团核心成员，参与组织东南大学首届环九龙湖自行车赛，两次参与组织 “先声之夜” 晚会（东南大学规模最大的电竞比赛）

科研与工作经历

- **针对加密硬件静态功耗的的侧信道攻击** 圣约翰斯，加拿大
  纽芬兰纪念大学博士科研项目 *2015 年 1 月 - 至今*

  摘要： 在针对加密硬件的攻击中，侧信道攻击已经被证明是一种有效的攻击方式。在很多著名的攻击算法中，动态功耗泄露都被用作为侧信道攻击的分析对象。随着芯片制作工艺的进步，工艺尺寸逐步缩小，静态功耗在总功耗中占的比例随之增大。在小于 100nm 的芯片工艺中这一变化尤为明显，因此静态功耗也可能成为潜在的侧信道攻击分析对象。在侧信道攻击算法中模板攻击是一种强有力的攻击方法。这种方法针对所有可能的密钥建立在随机输入情况下的统计模型，并将其与正确密钥在随机输入时的统计模型进行比较，以获取正确的密钥信息。我们提出了一类模板攻击算法，用于针对块加密算法进行静态功耗分析。我们所提出的模板攻击算法使用了在其它领域所使用的新的概率模型区分工具。

  - 用 Cadence 和 Synopsys 系列工具以及 45nm 库实现轻量级加密算法的硬件电路。设计流程包括使用 Verilog 实现 RTL 逻辑、使用 Synopsys Design Compiler 综合、使用 Cadence Encounter 布线以及使用 Cadence Virtuoso 进行晶体管级别的仿真。使用 Ocean 脚本对仿真电路的静态功耗进行测量记录以进行侧信道攻击。
  - 使用统计工具分析功耗波形的概率分布模型，所用统计工具包括：PCA、多元高斯分布、朴素贝叶斯法、核函数、相对熵、Jensen-Shannon distance 等。
  - 改进原有的模板攻击算法，将其成功应用在块加密的静态功耗上。改进了一系列影响该攻击方法可用性的问题。并将一些统计方法作为概率模型区分工具应用于模板攻击算法。
  - 在早期研究中用曲线拟合、线性规划等统计工具验证比特切片电路结构在小于 100nm 的芯片工具中的影响。
  - 使用 Python 实现各种模板攻击算法，并对功耗波形数据进行统计分析。
  - 部分成果已发表于会议 NECEC’15 和 MWSCAS’17，另有一篇论文正在 IEEE Transactions on Circuits and Systems I 审核中。
  - 该项目科研基金由加拿大自然科学与工程研究委员会（NSERC）提供。

- **使用模糊边缘检测的图像信息隐藏算法** 圣约翰斯，加拿大
  纽芬兰纪念大学课程项目 *2014* 年 *5* 月 *- 2014* 年 *11* 月

摘要： 图像信息隐藏技术可以将敏感信息隐藏在伪装图像中，从而保证将伪装图像发送给对方时其中的隐藏信息不被攻击者发现的方法。图像中的边缘部分通常含有较多的噪音，因此相比平滑的部分更加适合隐藏信息。我们提出了一种使用混合边缘检测的最低位比特信息隐藏算法。这个算法基于 W.-J. Chen 等人所提出的方法。我们的方法只需使用一个模糊逻辑，因此可以实现比原算法更快的运行效率。并且我们的方法对边缘像素的检测结果可以包含原算法的所有检测结果。同时在我们的测试中我们也证实我们的算法比原算法可以隐藏更多的信息，同时对伪装图像的破坏更少。

  - 提出了一种图像信息隐藏算法，使用模糊逻辑来寻找图像中的边缘，并将敏感信息隐藏在边缘像素的低比特位中。
  - 使用 Matlab 实现算法，并设计 GUI 以方便用户使用。
  - 成果已发表于会议 NECEC’14。

- **半同态加密算法的实现** 圣约翰斯，加拿大
  纽芬兰纪念大学硕士毕业设计项目 *2013* 年 *9* 月 *- 2014* 年 *4* 月

摘要： 同态加密所产生的密文具有特殊的性质，即对两个密文进行某个运算后对运算结果进行解密，所得的解密后明文对应等于两个密文的明文的相同运算结果。对任何运算均可以无限次数的实现同态性质的加密称为全同态加密，同态运算方式或次数有限的加密称为半同态加密。本项目目标为医学数据挖掘等实际应用搭建一个可用于保护隐私的加密框架。该加密框架将在数据统计中使用，因此需要满足加同态以及有限的乘同态的同态加密算法。本人参与学习并使用 Java 实现论文 A simple BGN-type cryptosystem from LWE 中所提出的半同态加密算法，实现密文的多次同态加法以及一次同态乘法。

  - 参与搭建系统的原型架构，以便将其应用在医学数据挖掘等场景中。
  - 使用 Java 实现半同态加密算法。

- **AES 算法的并行化实现** 圣约翰斯，加拿大
  纽芬兰纪念大学课程项目 *2013* 年 *1* 月 *- 2013* 年 *4* 月

  - 使用生产者/消费者模型进行并行处理，AES 算法使用 ECB 工作模式
  - 使用 Java 实现多线程并行算法。

- **Grain 密码家族的硬件实现** 圣约翰斯，加拿大
  纽芬兰纪念大学课程项目 *2013* 年 *1* 月 *- 2013* 年 *4* 月

  - 实现了 Grain-128 与 Grain-128a。

  - 使用 VHDL 实现算法，并使用 Quartus II 进行调试与编译。

- **助教** 圣约翰斯，加拿大
  纽芬兰纪念大学 *2014 年 1 月 - 至今*
  - 协助教授批改作业、辅导实验以及为课程准备幻灯片。曾担任如下课程助教：ENGI 8868/9877 Computer & Communications Security、ENGI 3861 Digital Logic、ENGI 7854/9804 Industrial Machine Vision 等等。
  - 曾由于在 2015 年 1 到 4 月的 ENGI 8868/9877 Computer & Communications Security 课程、2016 年 9 到 12 月的 ENGI 3861 Digital Logic 课程中的表现，获得课程教授寄来的感谢信。
- **软件工程师（实习）** 南京，中国
  途牛旅游网 *2011 年 10 月*
  - 前端开发实习，使用公司已有的 MVC 框架和 RPC 接口进行新系统的开发。
  - 项目包括 CRM 系统、富文本编辑器以及各种页面实现。
  - 使用技术：PHP、SQL、jQuery 以及 AJAX。
- **前端工程师** 南京，中国
  东南大学先声工作室 *2009 年 10 月 - 2011 年 6 月*
  - 先声工作室是下属于东南大学党委宣传部的学生工作室，负责为学校单位开发网络应用。
  - 在参与先声网站的开发管理期间，开发了 2010 年艺文频道、2011 年艺文频道。在项目中，主要负责 Linux 系统下 PHP 开发。其中，2010 年版本实现 PHP 频道网站的后台与 Java 下单点登录（SSO）系统的 Web Service 连接接口以及相关的加密处理。2011 年版本使用 ThinkPHP 框架，并在后台管理系统中使用 AJAX，优化了用户体验。
  - 使用技术：Linux、Apache server、PHP、MySQL、jQuery 以及 AJAX。
- **网站开发** 南京，中国
  东南大学计算机科学与工程学院暑期社会实践 *2010 年 7 月 - 2010 年 8 月*
  - 为计算机科学与工程学院题为《农民工的现状与思考》的暑期社会实践活动搭建网站，用于展示社会调研成果，进行网络宣传。
  - 因该项工作获得 2010 年东南大学暑期社会实践优秀个人称号。
  - 使用技术：PHP、MySQL、CSS 以及 HTML。

论文

- J. Xu and H. M. Heys, “Template Attacks Based on Static Power Analysis of Block Ciphers in 45-nm CMOS Environment,” *In Proc. of the IEEE Midwest Symposium on Circuits and Systems* (*MWSCAS’17*), Boston, USA, Aug. 2017.

- J. Xu and H. M. Heys, “Introduction to Static Power Analysis of Cryptographic Devices,” *In Proc. of the IEEE Newfoundland Electrical and Computer Engineering Conference* (*NECEC’15*), St. John’s, Canada, Nov. 2015.

- J. Xu and M. Shehata, “Image Steganography Using Fuzzy Edge Detector,” *In Proc. of the IEEE Newfoundland Electrical and Computer Engineering Conference* (*NECEC’14*), St. John’s, Canada, Nov. 2014.

- J. Xu and H. M. Heys, “Kernel-Based Non-Parametric Template Attacks Using Static Power,” IEEE Transactions on Circuits and Systems I 审稿中.

奖项荣誉

- 东南大学第三届嵌入式系统设计大赛校三等奖，2010 年 5 月。
- 东南大学第六届 RoboCup 机器人仿真大赛校三等奖，2009 年 10 月。
- 东南大学暑期社会实践优秀个人（因在《农民工的现状及思考》社会实践课题中负责网站开发和网络宣传），2010 年 12 月。
- 中国大学生艺术展演合唱比赛国家一等奖，2011 年 6 月.
- 东南大学计算机科学与工程学院杰出艺术活动奖学金，2010 年 10 月以及 2011 年 5 月。

培训资质

- **Machine Learning** 由 Coursera 授予，2017 年 2 月。
- **Stand & Deliver: Presentation Skills** 由纽芬兰纪念大学 Gardiner Centre 授予，2013 年 2 月。
- **Technical Writing** 由纽芬兰纪念大学 Gardiner Centre 授予，2013 年 2 月。
- **Essential Communication Skills for Professionals** 由纽芬兰纪念大学 Gardiner Centre 授予，2013 年 2 月。
- **系统集成项目管理工程师** 由工信部授予，2010 年。

组织经历

- 成员，国际会议 Selected Areas in Cryptography 2016（在加拿大主办的唯一的密码学国际会议）本地组委会，2015 年 6 月 - 2016 年 8 月。
- 宣传部副部长，东南大学计算机科学与工程学院，2009 年 10 月 - 2010 年 6 月。
- 学生成员，IEEE，2017。

技能

- **熟练：** Python、Matlab、数值计算库、Linux、LaTeX、Verilog、Cadence Virtuoso。
- **掌握：** C++、Java、git、Cadence Encounter、Synopsys Design Compiler、VHDL、PHP、SQL、CSS、HTML、jQuery。

语言能力

- 大学英语六级 547，托福 95，雅思 6.5

KaneX

Ph.D. Candidate

Research Interest

- Side-channel attacks on light-weight ciphers in lower-end cryptographic circuits.
- Application of modern statistical tools in side-channel attacks.

Education

- **Memorial University of Newfoundland** St. John's, Canada
  Ph.D. in Computer Engineering *May 2014 - December 2018*
  - Thesis: Static-Power-Based Side-Channel Attack of Cryptographic Devices
  - Supervisor: Howard M. Heys
  - GPA: 4.00/4.00
  - Courses: ASIC Design, Industrial Machine Vision
  - Fully funded by the supervisor and fellowship from School of Graduate Studies.
- **Memorial University of Newfoundland** St. John's, Canada
  Master of Applied Science in Computer Engineering *July 2012 - April 2014*
  - Final project: An Implementation of Homomorphic Encryption
  - Co-supervisors: Howard M. Heys and Saeed Samet
  - GPA: 3.71/4.00, 3rd ranking in compulsory courses
  - Courses: Computer Architecture, High-Performance Computer Architecture, Advanced Concurrent Programming, Embedded/Real-Time System Design, Advanced Digital Systems, et. al.
- **Southeast University** Nanjing, China
  Bachelor of Engineering in Computer Science and Technology *August 2008 - June 2012*
  - Activities & Societies: core member of university choir; involved in the arrangement of the 1st Southeast University Circling-Jiulong-Lake Bicycle Race; involved in the arrangement of Herald Night (the largest e-sport contest in Southeast University) twice.

Research and Work Experience

- **Static-Power-Based Side-Channel Attack of Cryptographic Devices** St. John's, Canada
  Ph.D. research project at Memorial University of Newfoundland *January 2015 - Current*

  Abstract: Side-channel attack has been proven to be an efficient tool in attacking cryptographic devices. Dynamic power leakage has been used as a source for side-channel attack by many well-known cryptanalysis algorithms. As process technology size shrinks, the relative amount of static power consumption increases accordingly, and reaches a significant level in sub-100-nm chips, potentially changing the nature of side-channel analysis. Template attack is a strong type of side-channel attack algorithm. It utilizes the distribution information for each possible key with random inputs, and compares it with the distribution information of the correct key, in order to recover information about the correct key. We propose a type of template attack we developed for static power analysis of block ciphers. This template attack uses new distinguishers which are previously used in other statistical scenarios.

- Used Cadence and Synopsys tools to design circuits for light-weight ciphers in 45-nm environment. The design process includes RTL Verilog logic, synthesis using Synopsys Design Compiler, P&R using Cadence Encounter, and transistor-level simulations using Cadence Virtuoso. The static power consumption of the simulated circuits is measured and recorded using Ocean scripts to carry out side-channel attacks.
- Used statistical tools such as PCA, multivariate Gaussian distributions, kernels, KL divergence, and JS distance to analyze the probability distribution model of power consumption traces.
- Modified the original template attack algorithm to successfully attack block ciphers using static power leakage. Addressed the issues that affect the practicability of template attacks. Proposed a few statistical tools that can be used as the distinguisher for template attacks.
- Used statistical tools such as curve fitting and linear regression in the earlier stage of research to verify the effect of bit-sliced circuit structure in sub-100-nm environment.
- Used Python to implement the template attack algorithms and perform statistical analysis of power trace data.
- Part of the work has been published in NECEC'15 and MWSCAS'17. There is another paper under the revision of IEEE Transations on Circuits and Systems I.
- This project is funded by the Natural Sciences and Engineering Research Council (NSERC) of Canada.

- **Image Steganography Using Fuzzy Edge Detector** St. John's, Canada
  Course project at Memorial University of Newfoundland *May 2014 - November 2014*

Abstract: Image steganography embeds secret message in cover images, in order to ensure that the secret message will not be discovered by the attacker when the image is sent to the receiver. The edges in an image usually contains more noise, hence making it more suitable for secret message embedding than the smooth area. We propose a least significant bit embedding algorithm using hybrid edge detector. The proposed algorithm is based on the work presented by W.-J. Chen et al. This algorithm has faster performance as it uses only one fuzzy edge detector. The detection result can include all the edge pixels detected by the original detectors. As for the embedded cover image, it has been proved in test results that our work achieves higher message capacity and better quality for cover image than the proposal by W.-J. Chen et al.

- Proposed an image steganography algorithm, which uses fuzzy logic to detect edges and hides information in the edges of an image.
- Used Matlab to implement the algorithm, the final implementation includes an GUI for easy use.
- The outcome is published in NECEC'14.

- **An Implementation of Homomorphic Encryption** St. John's, Canada
  M.A.Sc final project at Memorial University of Newfoundland *September 2013 - April 2014*

Abstract: Homomorphism means that the decrypted computation result of two ciphertexts is the same of the corresponding computation result of their two plaintexts. If a homomorphic encryption scheme satisfies Homomorphism for any computational operation and for any times of computation, then it is a fully-homomorphic encryption, otherwise it is a semi-homomorphic encryption (SHE) The main purpose of this project is to implement a homomorphic encryption system that can work as privacy preserving protocol for real-world application like medical care and business intelligence. This mainly consists of studying SHE, and implementing a SHE scheme proposed in *A simple BGN-type cryptosystem from LWE*, which satisfies homomorphism for multiple additions and one multiplication.

- Participated in building a prototype framework that is to be used in applications such as medical data mining.

- Used Java to implement a semi-homomorphic encryption algorithm.

- **A Parallel Implementation of AES** St. John's, Canada
  Course Project at Memorial University of Newfoundland *January, 2013 - April, 2013*
  - The producer/consumer model is used to implement parallelism, the AES algorithm works in ECB mode
  - Used Java to implement a multi-thread program.

- **Hardware Implementation of Grain Cipher Family** St. John's, Canada
  Course Project at Memorial University of Newfoundland *January, 2013 - April, 2013*
  - Grain-128 and Grain-128a are implemented in this project.
  - Used VHDL to implement the algorithms, and used Quartus II to debug and compile the source code.

- **Teaching Assistant** St. John's, Canada
  Memorial University of Newfoundland *January 2014 - Current*
  - Assisted marking, lab tutoring, and slides preparation of courses such as ENGI 8868/9877 Computer & Communications Security, ENGI 3861 Digital Logic, ENGI 7854/9804 Industrial Machine Vision et. al.
  - Received appreciation for the performance in assisting ENGI 8868/9877 Computer & Communications Security during the January - April semester in 2015 and in assisting ENGI 3861 Digital Logic during the September - Decemter semester in 2016.

- **Software Engineer, Intern** Nanjing, China
  Tuniu.com *October 2011*
  - Worked as a front-end developer, used existing MVC framework and RPC protocol to build projects.
  - Participated in projects including building the CRM system, rich-text editors, and website pages.
  - Technology: PHP, SQL, jQuery, and AJAX.

- **Front-End Engineer** Nanjing, China
  Herald Studio at Southeast University *October 2009 - June 2011*
  - Worked for a student organization that develops web applications for Southeast University.
  - Participated in the development of Literature 2010 and Literature 2011 sites. Mainly responsible for PHP developments in Linux environment. The Literature 2010 site uses WebService to connect with the Single-Sign-On protocol provided by Java server. A simple encryption protocol is implemented for the communication. The Literature 2011 site uses the ThinkPHP framework, and uses AJAX in its administration system for better user experience.
  - Technology: Linux, Apache server, PHP, MySQL, jQuery, and AJAX.

- **Website Developer** Nanjing, China
  Summer Social Practice at Southeast University *July 2010 - August 2010*
  - Built a website for the summer social practice named *The Current Situation and Thinking of Migrant Workers* conducted by the School of Computer Science and Engineering, in order to present and promote the outcome of this activity.
  - Granted Excellent Person Award by Southeast University for the contribution in this activity.
  - Technology: PHP, MySQL, CSS, and HTML.

Papers

- J. Xu and H. M. Heys, “Template Attacks Based on Static Power Analysis of Block Ciphers in 45-nm CMOS Environment,” *In Proc. of the IEEE Midwest Symposium on Circuits and Systems* (*MWSCAS’17*), Boston, USA, Aug. 2017.
- J. Xu and H. M. Heys, “Introduction to Static Power Analysis of Cryptographic Devices,” *In Proc. of the IEEE Newfoundland Electrical and Computer Engineering Conference* (*NECEC’15*), St. John’s, Canada, Nov. 2015.
- J. Xu and M. Shehata, “Image Steganography Using Fuzzy Edge Detector,” *In Proc. of the IEEE Newfoundland Electrical and Computer Engineering Conference* (*NECEC’14*), St. John’s, Canada, Nov. 2014.
- J. Xu and H. M. Heys, “Kernel-Based Non-Parametric Template Attacks Using Static Power,” Under review by IEEE Transactions on Circuits and Systems I.

Awards and Honors

- 3rd Prize in the 3rd Embedded System Design Contest, Southeast University, May 2010.
- 3rd Prize in the 6th RoboCup Robotic Simulation Competition, Southeast University, October 2009.
- Excellent Person Award in summer social practice (for the work in website development), Southeast University, December 2010.
- 1st Prize in National University Art Exhibition - Chorus Contest, China, June 2011.
- Scholarship for outstanding art activities, School of Computer Science and Engineering at Southeast University, October 2010 & May 2011.

Certificates

- **Machine Learning:** issued by Coursera, February 2017.
- **Stand & Deliver: Presentation Skills:** issued by Gardiner Centre, Memorial University of Newfoundland, February 2013.
- **Technical Writing** issued by Gardiner Centre, Memorial University of Newfoundland, February 2013.
- **Essential Communication Skills for Professionals:** issued by Gardiner Centre, Memorial University of Newfoundland, February 2013.
- **System Integration Project Management Engineer:** issued by Ministry of Industry and Information Technology, China, 2010.

Organizations

- Member, Local Arrangement Committee for Selected Areas in Cryptography 2016 (The only international conference in cryptography hosted in Canada), June 2015 - August 2016.

- Vice Minister of Propaganda Department, School of Computer Science and Engineering of Southeast University, October 2009 to June 2010.
- Student Member, IEEE, 2017.

Skills

- **Advanced:** Python, Matlab, numerical libraries, Linux, LaTeX, Verilog, Cadence Virtuoso.
- **Intermediate:** C++, Java, git, Cadence Encounter, Synopsys Design Compiler, VHDL, PHP, SQL, CSS, HTML, jQuery.

Language Proficiency

- CET-6 547, TOEFL 95, IELTS 6.5